IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF:
Apple iPhone SE, serial number FFMF616GPLJN, and a Samsung Galaxy S9, IMEI 353305098516707,
Currently located at FBI Richmond, 1970 E Parham Road, Richmond, VA 23228

UNDER SEAL
Case No. 3:21-sw-155

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Alicia A. Cruz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since 2007. I am currently assigned to the Richmond Division, Fredericksburg Resident Agency and have been since 2019. While employed with the FBI, I have investigated federal criminal violations related to child exploitation and child pornography. I have participated in investigations in which perpetrators have used computers to commit violations involving the sexual exploitation of children. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of

child pornography (as defined in 18 U.S.C. §2256) in all forms of media. These forms of media include computer media, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including production of child pornography, in violation of 18 U.S.C. § 2251(a), and distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252(a). I have also participated in numerous search warrants that involved child exploitation and/or child pornography offenses.

3. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7) and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is an Apple iPhone SE, serial number FFMF616GPLJN and a Samsung Galaxy S9, IMEI 353305098516707, hereinafter the "Devices." The Devices are currently located at FBI Richmond Field Office, Evidence Control Room, 1970 E. Parham Road, Richmond, VA 23228.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. In the days leading up to September 7, 2021, a Federal Bureau of Investigation ("FBI") Washington Field Office ("WFO") Task Force Officer ("TFO") was acting in an

undercover ("UC") capacity, as part of the Metropolitan Police Department-Federal Bureau of Investigation ("MPD-FBI") Child Exploitation Task Force, operating out of a satellite office in Washington, D.C. In that capacity, the UC entered a private KIK[1] group. This group is known to the UC as a place where people meet to discuss their sexual interest in children, and to trade images and videos that depict the sexual abuse of children.

8. In this private KIK group, the UC observed a KIK user utilizing the KIK name usedforlife1 with the display name of Josh Lopez, subsequently identified as Josh Lopez ("Lopez"). The undersigned initiated a private KIK chat with this subject. During the course of the chat, Lopez stated that he was a 23-year-old male residing in Virginia with his wife. Lopez also stated that he has access to a 2-year-old, whom he claimed to be sexually abusing. During this point in the KIK chat, Lopez sent clothed images of this purported 2-year-old to the UC. In one of these images, Lopez's face is visible, and he is holding a toddler.

9. As the KIK chat progressed, the UC told Lopez that he has an 8-year-old daughter, whom he was sexually abusing. Lopez asked the UC if he could engage in sex acts with the UC's purported 8-year-old daughter. Lopez then provided the UC with his cellular number, and he began communicating with the UC using both KIK and text messages.

10. The following is a portion of the chat that the UC and Lopez engaged in on September 7, 2021, where Lopez describes sexually abusing the child:

Lopez: Ive made her suck it and tried to fuck her

UC: That's so hot I bet her little pussy looks so good

---

[1] KIK is an instant messaging mobile application where one can transmit and receive messages, photos, and videos. Users can communicate privately with other users or in groups.

Lopez: yes it does, do you have any naked pictures of her

UC: Let me look, do you have any naughty pictures of her too?

Lopez: I can get them but you will have to wait

UC: Where are they on another devise?

Lopez: No I have to take them

UC: Oh, have you ever taken any in the past

Lopez: Yeah sorry, no

UC: Oh well don't worry about it if you don't take pics lol

Lopez: I will

UC: U ever get pics from any other real dads

Lopez: Yes

UC: Mmm how young and did they send naughty ones

Lopez then sent the UC a zoomed-in image, depicting what appears to be the nude vagina and pubic area of a pubescent girl. Lopez informed the UC that the girl depicted in this image was 16 years old.

11. As the chat continued, on September 9, 2021, Lopez agreed to meet the UC and his purported 8-year-old daughter in the District of Columbia on September 13, 2021. The discussed purpose of the meeting was for Lopez to sexually abuse the minor. The UC attempted to contact Lopez via text message on September 11, 2021, to confirm the meeting time and location. Lopez did not respond to the UC's message and did not communicate again with the UC until September 17, 2021.

12. When Lopez resumed the chat with the UC, he stated that he had been really busy. He also stated that he accidently deleted the chats he had engaged in with the UC. Lopez informed the UC that he was interested in watching the UC sexually abuse his 8-year-old daughter. Lopez asked the UC for pictures of his daughter. In response, the UC sent Lopez a clothed image depicting his purported daughter.[2]

13. On September 22, 2021, Lopez contacted the UC via KIK instant messenger. The following is a portion of that chat:

Lopez: Got a pic

UC: ?

Lopez: of her puss

UC: You do? Of who?

Lopez: [a child][3]

UC: mmm no way which one

Lopez then sent the UC two images, each depicting a toddler girl who Lopez said was the previously discussed 2-year-old. The first image depicts a close-up view of a toddler's bare vagina. An adult male's hand is visible, and he is using his thumb and index finger to spread the toddler's vagina open. The child's face is not visible in this image, but the little girl is shown wearing a pink shirt that is frayed on the bottom. The second image depicts a close-up view of the same child's bare vagina. After sending these images, Lopez told the UC that he put his penis inside the toddler's mouth, and that he ejaculated into her mouth.

---

[2] The image the UC sent to Lopez did not depict a real child.

[3] This portion of the chat has been changed to avoid identifying a minor child.

14. During the chat on September 22, 2021, Lopez informed the UC that he took the images earlier that day, and that he has been sexually abusing the 2-year-old for one year. When communicating with the UC using KIK, Lopez asked the UC if he would live video stream the UC having sexual intercourse with his purported 8-year-old daughter. When explaining his request, Lopez stated, "I want you to have her suck it than going to fuck her pussy and cum in it.

15. During the course of the investigation, law enforcement in Washington, D.C. learned that Lopez was also communicating with, and sending the same images to, another law enforcement officer, acting in an undercover capacity, in a different state ("UC2"). Lopez sent UC2 photographs of a toddler girl that he also claimed to have access to. A Facebook page with the display name "Joshua Lopez" was also located. This Facebook page contained a photo depicting what appears to be the same individual as the individual depicted in the profile picture of the Kik account that Lopez was using to communicate with the UC. Additionally, there is a photograph of a young girl who has a distinctive mole on her cheek on the Joshua Lopez Facebook page. This appears to be the same child as the toddler depicted in the images that Lopez sent to the UC in September of 2021.

16. In addition, FBI Fredericksburg RA learned that Lopez was also communicating with, and sending the same images to, another law enforcement officer acting in an undercover capacity, in a different state ("UC3"). UC3 began conversing in a KIK group known to UC3 as a place where people meet to discuss their sexual interest in children, and to trade images and videos that depict the sexual abuse of children.

17. In this private KIK group, UC3 observed a KIK user utilizing the KIK name usedforlife1 with the display name of Josh Lopez, subsequently identified as Josh Lopez ("Lopez"). UC3 and Lopez engaged in a private KIK chat where Lopez told UC3 that he was a

23-year-old male residing in Virginia. Lopez told UC3 that he has access to a 2-year-old child, whom he claimed to be sexually abusing.

18. On September 8, 2021 UC3 told Lopez that he has an 11-year-old daughter and Lopez asked UC3 if he could send pictures of his daughter. UC3 said he would not because Lopez was not legit. On September 9, 2021 Lopez sent UC3 two videos of prepubescent females in sexual acts. On September 22, 2021, Lopez sent UC3 two images, each depicting a toddler girl. Lopez told UC3 that the images were of the previously discussed 2-year-old. The first image depicts a close-up view of a toddler's bare vagina. The second image depicts a close-up view of a toddler's bare vagina. In this image an adult male's hand is visible, and he is using his thumb and index finger to spread the toddler's vagina open. The child's face is not visible in this image, but the little girl is shown wearing a pink shirt that is frayed on the bottom. Lopez told UC3 that he has sexually abused the child by doing "pussy fuck bj" and "I eat her pussy before I had to leave." Lopez sent UC3 clothed images of what he said was him with the 2-year-old. In one of these images, Lopez's face is visible, and he is holding a female toddler. In another image half of Lopez's face is visible and he is holding what appears to be the same female toddler.

19. During the chat on September 22, 2021, Lopez started asking UC3 about sexual acts related to UC3's purported 11-year-old daughter. During the chat, Lopez asked UC3, "Why you want me to fuck her pussy" and "Do u want to try to [sic] dicks in her pussy".

20. On September 23, 2021, a state search warrant was executed on Lopez's residence. Lopez was interviewed by VSP and the FBI. Lopez said that his screen name on KIK Messenger is usedforlife1. Lopez said that he took the photos on September 22, 2021 of the 2-year-old's vagina and sent them to people on KIK. Lopez stated that he used his phone, the

iPhone SE, for this purpose. Lopez also stated that he sexually touched the 2-year-old with his hands and wanted to perform oral sex on the child. Lopez said that he had been having sex with a 16-year-old for the past two years. Lopez stated that he had images of the 16-year-old's vagina and breasts on his phone.

21. During execution of the state search warrant by the Northern Virginia Internet Crimes Against Children Task Force and the FBI Fredericksburg Resident Agency on September 23, 2021, the Devices were located in Lopez's residence in the bedroom. Lopez identified the Devices as his and the iPhone SE as his primary phone. A forensic triage of the iPhone SE was performed on scene. Additionally, during the interview of Lopez, he stated that he had deleted recent photos of child pornography from his iPhone SE but that he could go into the deleted photos folder to recover the child pornography images if he wanted. For purposes of forensic extraction, deleted photos on an iPhone have a 30-day preservation period in the deleted files folder before they are permanently deleted from the device. To attempt to recover these deleted images, a VSP agent, acting pursuant to the previously obtained state search warrant, used forensic imaging tools to extract a forensic image of the iPhone SE in an attempt to recover any deleted images before they were permanently lost. This extraction has not been reviewed. After obtaining the extraction, a VSP agent then opened the phone and manually moved the deleted images from the deleted files folder to the phone's storage library to attempt to ensure that all deleted images were preserved.

22. The Devices are currently in the lawful possession of the FBI. Initially Virginia State Police took possession of the devices during the execution of the search warrant on September 23, 2021. On September 30, 2021 the devices were turned over to the FBI Fredericksburg Resident Agency by Virginia State Police. Therefore, while the FBI might

already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

23. The Devices are currently in storage at FBI Richmond Field Office Evidence Control Room. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing

dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

25. Based on my training, experience, and research, I know that the Devices are "smart phones" which have capabilities that include most, if not all, of those described in paragraph 19. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices, and how the devices were used in furtherance of the offenses under investigation.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to receive or distribute child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Alicia Cruz
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before
me on October 8, 2021:

/s/ MRC

Mark R. Colombell
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Apple iPhone SE, serial number FFMF616GPLJN and a Samsung Galaxy S9, IMEI 353305098516707, hereinafter the "Devices." The Devices are currently located at FBI Richmond Evidence Control Room, 1970 E. Parham Road, Richmond, VA 23228.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be Seized

1. All records and information relating to possible violations of the following criminal offenses: production of child pornography, in violation of 18 U.S.C. § 2251(a), and distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252(a) including:

   a. Any and all visual depictions of minors;

   b. Any and all communications with minors;

   c. Any and all address books, names, and lists of names and addresses of minors;

   d. Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;

   e. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;

   f. Records and information relating to Kik username usedforlife1 and any related Kik accounts.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. For any device or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "DEVICE"):

   a. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as

logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the DEVICE of other storage DEVICE or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

f. evidence of the times the DEVICE was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;

h. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;

i. records of or information about Internet Protocol addresses used by the DEVICE;

j. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review